

Virtual CIO - Executive Summary - Backups

How great it feels to go to sleep at night knowing your data has been backed up and all of your accounting and business files are protected unless something goes wrong. Unfortunately that blanket of security that you sleep under may be full of holes. Twice in the last 4 months I've heard of companies attempting to restore their data only to find out that their backups haven't been working for years. Their backups had been incorrectly reporting a successful backup while an error had gone unreported.

You might be able to rest a little easier if you learned that these disasters struck a local convenience store. Unfortunately that isn't the case. Both organizations have revenues in the millions - one in the hundreds of millions. If your backup is very fast, beware.

If you haven't tested your backup - you don't have a backup.

Let's take a look at some of the best practices of backups - most using very inexpensive software.

Full, Incremental, Image, Files, Web-based & Replication

First we need to address some backup terminology. Backups are either 'full' or 'incremental' and 'image' or 'files'. An image backup is just that, it is an image of every byte and bit stored on your disk drive. If you have one of these you won't need to reinstall any software, your backup is a clone of your storage. A restore of an image backup taken with Norton's Ghost or Clonezilla and a few others. By definition, an image or clone backup is a full backup - it backs up everything.

As an alternative to an image backup, you can just back up certain parts of your hard disk. If you have another computer standing by with all of the same software installed on it or if you are comfortable with re-installing all of your software then a file backup will save you a lot of time. Many people only backup their 'My Documents' folder. A good software - I've heard - to look at for this is Cobian Backup which in version 8 is free OpenSource software.

With the new backup architecture that backs up a disk to another disk, this incremental backup is becoming obsolete in certain circumstances. An incremental backup only backs up what has changed since the last backup. So if you took a full backup, an incremental backup would only backup what has changed since the last backup. If you only changed two files, then only two files would be in the backup.

There is another family of backups that makes copies of your changes on the fly. On my system for example, every file that I write to My Documents is copied hourly to another disk on the network. So my exposure of data loss is never more than an hour. GoodSync is an excellent example of this technology.

Offsite Storage

Once common shortfall of a good backup strategy is that people don't vault their backups - take them offsite. In a perfect world, as soon as the backup was completed, it would be taken off site and put in a safe deposit box. So it does get me nervous when I see the backup tape left in the tape drive which is connected to the computer being backed up. I don't think a fire would respect the backup and only burn the disk drive. The important thing isn't getting it to the bank, it is getting the backup to the place where a separate disaster would have to occur to destroy the original and the backup. The good news is that there are a number of companies offering an internet based backup where you can backup your data over the internet to an offsite storage facility - very secure. While there are a number of these you can look at, I'd recommend Mozy be at the top of your list. It is an EMC company - big name in storage - and it's free for 2G or less of personal storage.

There is one more type of backup but it isn't used very much in the small business world. It is the 'log file' where every transaction written to the database is backed up to allow you to restore the database to the instant the data loss occurred.

Multiple Generations

The last backup term that we want to cover is generations. I've seen cases where a backup strategy for a company was executed perfectly except for the 'single point of failure' which we'll cover in another lesson. If you only have one backup,

then you're relying on never having a scratched DVD or wrinkled tape. I recommend 3 generations - which says three things have to fail before you've lost data. Note: In some circumstances the criticality of the data will suggest that five generations be taken - this should get you to six 9's of reliability - i.e. 99.9999%

isResearch's Top 8 List for Backups

- Develop a strategy and train people on how to execute that strategy.
- Create a backup log. If it doesn't get recorded it might not happen.
- Keep multiple generations - the most current offsite.
- Test, Test, Test! Never assume that it's working. Do a full test at least once a year.
- Secure the backup. You have all kinds of passwords on your system but if someone has access to your backup they have everything. This includes the point at which you dispose of the media - clean it first.
- Schedule the backup so it is convenient. You don't want someone staying late to do it - it might not get done.
- Rotate your media if it is prone to wearing out. If you're backing up to a 10 year old tape, you might be in trouble.
- Build a library and label the media. It doesn't do much good if you don't know what you have.

Scary thought of the day: If you take one backup a month and put it in your car you will more secure than 90% of US businesses.